

849



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/438,342	11/11/1999	GREGORY G. ROSE	PA990055	9169

23696 7590 04/14/2004

Qualcomm Incorporated  
Patents Department  
5775 Morehouse Drive  
San Diego, CA 92121-1714

EXAMINER

MCARDLE, JOSEPH M

ART UNIT	PAPER NUMBER
----------	--------------

2132

10

DATE MAILED: 04/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/438,342

Applicant(s)

ROSE, GREGORY G.

Examiner

Joseph McArdle

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 1/15/2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-4, 8-10, 14-16, 20-22, 26, 27 and 29 is/are rejected.
- 7) ☒ Claim(s) 5-7, 11-13, 17-19, 23-25, 28, 30 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 November 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

**DETAILED ACTION**

1. Applicant's arguments with respect to claims 1-30 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 14 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 14, which is dependent from claim 2, only recites "comprising" rather than "further comprising". The examiner notes that the limitation set forth under claim 2 is effectively negated by having claim 14 (which is dependant on claim 2) only recite "comprising" rather than "further comprising."

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 1, 2, 27, and 29 are rejected under 35 U.S.C. 102(a) as being anticipated by the "ATM security specification version 1.0" (hereinafter referred to as the "ATM security

reference"). In regards to claim 1, the ATM security reference discloses a design on page 141-142, paragraph 6.4.4 that pertains to cryptographic synchronization (synchronizing a stream cipher). It is further disclosed in paragraph 6.4.4 that to establish synchronization, an encryptor (transmission source) transmits a resync message to a decryptor (reception site) that includes the encryptor's state vector (control set of numbers). It is further disclosed in the aforementioned location that the decryptor will use the state vector in order to perform resynchronization (by using the state vector to determine the current state of the cipher). These disclosures meets the exact limitations set forth under claim 1, which call for transmitting a control set of numbers (state vector) indicating a current state of the stream cipher at the transmission source and using the control set of numbers (state vector) to determine the current state of the cipher.

6. In regards to claim 2, The ATM security reference further discloses in figure 39 on page 143 and in paragraphs 6.4.6.1.2 and 6.4.6.3 on pages 144 and 145 respectively that the state vector (which is transmitted from the transmission source) includes a sequence number (cycle number) indicating when and how the LSFR is updated (or clocked). This disclosure meets the exact limitations set forth under claim 2, which calls for having a control set of numbers (state vector) comprising a cycle number (sequence number).

7. In regards to claims 27 and 29, the ATM security reference discloses a design on page 141-142, paragraph 6.4.4 that pertains to cryptographic synchronization (synchronizing a stream cipher). It is further disclosed in paragraph 6.4.4 that to establish synchronization, an encryptor (transmission source) transmits a resync message to a decryptor (reception site) that includes the encryptor's state vector (control set of numbers). It is further disclosed in the aforementioned location that the decryptor will use the state vector in order to perform resynchronization (by using the state vector to determine the current state of the cipher). The ATM security reference further discloses in figure 39 on page 143 and in paragraphs 6.4.6.1.2 and 6.4.6.3 on pages 144 and 145 respectively that the state vector (which is transmitted from the transmission source) includes a sequence number (cycle number) indicating when and how the LSFR is updated (or clocked). The ATM security reference finally discloses in paragraph 6.4.6.5 on page 146 how a jump number (representative of the offset between the ciphers of transmission source and the reception site) is also included in the state vector that is transmitted from the encryptor (transmission source) to the decryptor (reception site). It is this transmitted state vector, which includes the jump number, that allows the reception site to synchronize its cipher with the output of the transmission site's LFSR. These disclosures meet the limitations set forth under claims 27 and 29, which call for determining an offset from the transmission site's LFSR and transmitting it to a reception site so that the reception site can properly synchronize its cipher

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference in view of Raith (5546464). The ATM security reference disclosed above meets all of the aforementioned limitations of claim 2 above. However, the ATM security reference does not mention transmitting from a mobile station to a base station. Raith discloses in column 12, lines 24-28, that synchronization can be obtained when transmissions are made in either direction between mobile stations and base stations. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Raith's teachings on the use of transmitting between mobile stations and base stations into the ATM security reference in order to achieve a design that is capable of transmitting from a mobile station to a base station.

10. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference in view of Jansen (6587562). The ATM security reference disclosed above meets all of the aforementioned limitations of claim 2 above. However, the ATM security reference does not mention having polynomials of various degree for determining the current state of the stream cipher. Jansen discloses in column 6, lines

22-41, that linear feedback shift registers use polynomials of various degree and that these polynomials represent the bit shifting operations that occur during a ciphering process. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Jansen's teachings, pertaining to the use of various degree polynomials, into the ATM security reference in order to achieve a design that is capable of determining the current state of the stream cipher by employing the use of a polynomial that represents the bit shifting operations that occur during the ciphering process.

11. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference in view of Bright (4893339). In regards to claims 8 and 9, The ATM security reference described above meets all of the aforementioned limitations of claim 2. However, the ATM security reference does not mention transmitting the encrypted data stream to a plurality of recipients whereby each recipient uses the control data containing the cycle numbers to determine a different current state of the stream cipher. Bright discloses in column 3, lines 12-24, a transmission system that comprises a base station and a plurality of remote units. Bright further discloses in column 4, lines 27-35, that a plurality of synchronization signals may be used, each of which may indicate a particular group of recipients. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Bright's teachings on the use of transmitting to a plurality of recipients into the ATM security reference design in order to achieve a design that transmits encrypted data from a

source to a plurality of recipients, whereby each recipient uses the control data contained within the encrypted data to determine a different current state of the stream cipher.

12. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference in view of Finkelstein (5060265). In regards to claim 14, The ATM security reference disclosed above meets all of the aforementioned limitations set forth under claim 2. However, the ATM security reference makes no mention of including a stutter number, for the purposes of introducing non-linearity into the output of the LFSR, in the control set of numbers that is to be transmitted. Finkelstein teaches in column 1, lines 57-67 through column 2, lines 1-12 that cryptosystems weakness is caused by the LSFR's linearity. Finkelstein further teaches in the aforementioned location that it would be advantageous to provide a way to introduce non-linearity into the LSFR's output sequence for the purpose of making the LSFR robust against a cryptographic attack. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Finkelstein's teachings on the needs and advantages of introducing non-linearity into the output of a LSFR into the ATM security reference in order to achieve a design that allows a stutter number (which introduces non-linearity into the system) to be included in and transmitted with the control set of numbers.

13. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference and Bright as applied to claim 8 above, and further in view of Jansen.



The ATM security reference-Bright combination disclosed above meets all of the aforementioned limitations of claim 8 above. However The ATM security reference-Bright combination does not mention having polynomials of various degree for determining the current state of the stream cipher. Jansen discloses in column 6, lines 22-41, that linear feedback shift registers use polynomials of various degree and that these polynomials represent the bit shifting operations that occur during a ciphering process. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Jansen's teachings, pertaining to the use of various degree polynomials, into The ATM security reference-Bright combination in order to achieve a design that is capable of determining the current state of the stream cipher by employing the use of a polynomial that represents the bit shifting operations that occur during the ciphering process.

14. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference-Finkelstein combination as applied to claim 14 above, and further in view of Raith. The ATM security reference-Finkelstein combination disclosed above meets all of the aforementioned limitations of claim 14 above. However, the ATM security reference-Finkelstein combination does not mention transmitting from a mobile station to a base station. Raith discloses in column 12, lines 24-28, that synchronization can be obtained when transmissions are made in either direction between mobile stations and base stations. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Raith's teachings on the use of

transmitting between mobile stations and base stations into the ATM security reference-Finkelstein combination in order to achieve a design that is capable of transmitting from a mobile station to a base station.

15. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference-Finkelstein combination as applied to claim 14 above, and further in view of Jansen. The ATM security reference-Finkelstein combination disclosed above meets all of the aforementioned limitations of claim 14 above. However, the ATM security reference-Finkelstein combination does not mention having polynomials of various degree for determining the current state of the stream cipher. Jansen discloses in column 6, lines 22-41, that linear feedback shift registers use polynomials of various degree and that these polynomials represent the bit shifting operations that occur during a ciphering process. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Jansen's teachings, pertaining to the use of various degree polynomials, into the ATM security reference-Finkelstein combination in order to achieve a design that is capable of determining the current state of the stream cipher by employing the use of a polynomial that represents the bit shifting operations that occur during the ciphering process.

16. Claims 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference-Finkelstein combination as applied to claim 14 above, and further in view of Bright. The ATM security reference-Finkelstein combination described

above meets all of the aforementioned limitations of claim 14 above. However, the ATM security reference-Finkelstein combination does not mention transmitting the encrypted data stream to a plurality of recipients whereby each recipient uses the control data containing the cycle numbers to determine a different current state of the stream cipher. Bright discloses in column 3, lines 12-24, a transmission system that comprises a base station and a plurality of remote units. Bright further discloses in column 4, lines 27-35, that a plurality of synchronization signals may be used, each of which may indicate a particular group of recipients. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Bright's teachings on the use of transmitting to a plurality of recipients into the ATM security reference-Finkelstein combination design in order to achieve a design that transmits encrypted data from a source to a plurality of recipients, whereby each recipient uses the control data contained within the encrypted data to determine a different current state of the stream cipher.

17. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference-Finkelstein-Bright combination as applied to claim 20 above, and further in view of Jansen. The ATM security reference-Finkelstein-Bright combination disclosed above meets all of the aforementioned limitations of claim 14 above. However, the ATM security reference-Finkelstein-Bright combination does not mention having polynomials of various degree for determining the current state of the stream cipher. Jansen discloses in column 6, lines 22-41, that linear feedback shift registers

use polynomials of various degree and that these polynomials represent the bit shifting operations that occur during a ciphering process. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Jansen's teachings, pertaining to the use of various degree polynomials, into the ATM security reference-Finkelstein-Bright combination in order to achieve a design that is capable of determining the current state of the stream cipher by employing the use of a polynomial that represents the bit shifting operations that occur during the ciphering process.

18. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over the ATM security reference in view of Finkelstein. In regards to claim 26, the ATM security reference discloses a design on page 141-142, paragraph 6.4.4 that pertains to cryptographic synchronization (synchronizing a stream cipher). It is further disclosed in paragraph 6.4.4 that to establish synchronization, an encryptor (transmission source) transmits a resync message to a decryptor (reception site) that includes the encryptor's state vector (control set of numbers). The aforementioned location also discloses that the decryptor will use the state vector in order to perform resynchronization (by using the state vector to determine the current state of the cipher). The ATM security reference further discloses in figure 39 on page 143 and in paragraphs 6.4.6.1.2 and 6.4.6.3 on pages 144 and 145 respectively that the state vector (which is transmitted from the transmission source) includes a sequence number (cycle number) indicating when and how the LSFR is updated (or clocked). These disclosures meet the limitations set forth under claim 26, which call for transmitting a control set of numbers,

including a cycle number (state vector) indicating a current state of the stream cipher at the transmission source and using the control set of numbers (state vector) to determine the current state of the cipher at the reception site. However, the ATM security reference makes no mention of including a stutter number, for the purposes of introducing non-linearity into the output of the LFSR, in the control set of numbers that is to be transmitted. Finkelstein teaches in column 1, lines 57-67 through column 2, lines 1-12 that cryptosystems weakness is caused by the LSFR's linearity. Finkelstein further teaches in the aforementioned location that it would be advantageous to provide a way to introduce non-linearity into the LSFR's output sequence for the purpose of making the LSFR robust against a cryptographic attack. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Finkelstein's teachings on the needs and advantages of introducing non-linearity into the output of a LSFR into the ATM security reference in order to achieve a design that allows a stutter number (which introduces non-linearity into the system) to be included in and transmitted with the control set of numbers to the reception site where they will be used to determine the current state of the cipher.

***Allowable Subject Matter***

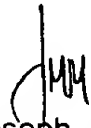
19. Claims 5-7, 11-13, 17-19, 23-25, 28, and 30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

**Conclusion**

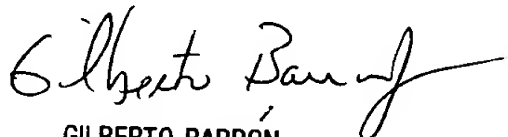
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph McArdle whose telephone number is (703) 305-7515. The examiner can normally be reached on Weekdays from 8:00 am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Joseph McArdle  
Examiner  
Art Unit 2132

jmm

  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100